UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,522	07/02/2003	Liqun Chen	B-5153 621074-2	4783

7590 06/18/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/613,522	CHEN ET AL.	
	Examiner	Art Unit	
	SHANTO M Z ABEDIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 19-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 19-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/28/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the **APPEAL BRIEF** filed on 04/07/2008. Finality of the previous office action is withdrawn, and subsequently this action is made NON-FINAL.

2. The examiner's note: Upon further examinations of claims 1-11 and 19-24, new grounds of rejection are found, and presented in this office action.

3. Claims 1-11 and 19-24 are pending in the application.

4. Claims 1-11 and 19-24 have been rejected.

Response to Arguments

5. The applicant's arguments regarding previous 35 USC 103 type rejections are fully considered, however, moot in view of new grounds of rejection presented in this office action.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-11 and 19-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1-7 and 19-21, they recite limitations "computing **first, second and third verification parameters** as the product of second secret with said shared secret, the second element and the first element **respectively**". However, it is not clear whether such parameters are representative of three different products, or whether only the first parameter is a product of second

secret with said shared secret, and second and third verification parameters are just second and first elements respectively! Therefore, meets and bounds of the claims are unclear.

As best understood, the examiner interpreted product of second secret with said shared secret as first verification parameter; and the second element as second verification parameter, and the first element as third verification parameter.

Regarding claims 8-11 and 22-24, they recite limitations "receiving in respect of the second party **both** an identifier string, and first, second and third verification parameters." However, it is not clear what is such 'both' is indicative of – since ordinarily, 'both' is followed by two different elements/ objects, on the contrary, there are four different elements are recited after 'both'.

Regarding claims 6-11 and 22-24, they recite limitations such as:

"carrying out a first check:

P (third verification parameter, computed second element)= ***P***(first element, second verification parameter)

carrying out a second check:

P(first element, first verification parameter)= ***P***(first product, second verification parameter)"

However, nothing else mentioned about what actually checked after the phrase "carrying out a first check:" or "carrying out a second check" – carrying out phrases simply followed by an equation/ equality type statements or functions. Is the equality of both sides of such statement or

functions are checked? Therefore, it is not clear what actually the applicant is trying to claim, and claim languages are considered unclear in their scope.

As best understood, the examiner interpreted, equality of such functions are checked by those first and second checking.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-11 and 22-24 are rejected under 35 USC 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claims 1-5, they are directed to a method. However, claim languages merely recite mathematical algorithm steps, and manipulation of mathematical/ abstract ideas, or speculative/ intended use of such mathematical results. Claim languages does not relate the claimed invention to any particular practical application. See MPEP 2106.02

In practical terms, claims define nonstatutory process if they:

- Consist solely of mathematical operations without some claimed practical application (i.e., executing a "mathematical algorithm"); or

- Simply manipulate abstract ideas, e.g., a bid (*Schrader,* 22 F.3d at 293-94, 30 USPQ2d at 1458-59) or a bubble hierarchy (*Warmerdam,* 33 F. 3d at 1360, 31 USPQ2d at 1759), without some claimed practical application.

Claim languages only recites mathematical operations, and further fails to disclose any practical application. Claim languages merely recite speculative/ abstract ideas or use of mathematical results such as " ..for use by the third party in proving the association between the first and second parties" instead of actually performing the step(s) of such 'proving' . Therefore, claim languages are considered to be directed to nonstatutory subject matter.

Regarding claims 6-7, they are directed to a method. However, claim languages merely recite mathematical algorithm steps/ checks, and manipulation of mathematical/ abstract ideas, or speculative/ intended use of such mathematical results. Claim languages does not relate the claimed invention to any particular practical application. See MPEP 2106.02

Although claim languages recite" the association between the first and second parties being treated as verified if both checks are passed", no practical application (besides mathematical steps/ checks) is actually performed at the end, such as an actual verification process is not claimed. Therefore, claim languages are considered to be directed to nonstatutory subject matter.

Regarding claims 8-11. they are rejected applying as above rejecting claims 1-7, furthermore, they are directed to a method. However, claim languages merely recite mathematical algorithm steps/ checks, and manipulation of mathematical/ abstract ideas, or speculative/ intended use of such mathematical results. Claim languages does not relate the claimed invention to any particular practical application. See MPEP 2106.02

Although claim languages recite" the association between the first and second parties being treated as verified if both checks are passed", no practical application is actually performed, such as

an actual verification process is not claimed. Furthermore, merely receiving mathematical values/ products does not result in any practical application, does not necessarily tie the mathematical products to an practical application. Therefore, claim languages are considered to be directed to nonstatutory subject matter.

Regarding claims 22-24, they are directed to an apparatus comprising means plus functions. However, according to the specification (please see Par 0069 and 0117), all of the claimed "means for" can be optionally implemented in computer program or software alone. Therefore, claimed invention is considered to be non-statutory as being directed to a program per se product. See MPEP 2106.01

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-5, 8-11 and 19-24 are rejected under 35 USC 103 (a) as being unpatentable over Gentry et al' 554 (US 2003/ 0182554 A1) in view of Boneh et al (US 2003/0081785A1) further in view of Gentry et al' 885 (US 2003/0179885A1).

Regarding claims 1, Gentry et al '554 discloses a method/ computer program product of enabling a third party to verify an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second party computer entity, acting on behalf of the second party:

receives a shared secret (Fig 4: step 414: shared secret g^{ab}, or Fig 5: interactive shared secret abP) provided by the first party as the product of a first secret and the second element (Fig 4,5; Par 0024, 0030, 0033; receiving interactive shared secret elements/ component from the first entity);

computes first (Fig 4, Fig 5; symmetric key from g^{ab}, or abP), second (Fig 4, Fig 5; second random element b) and third (Fig 4, Fig 5; first intermediate shared secret $g^{a,}$ or aP) verification parameters as the product of a second secret with said shared secret (Fig 4, Fig 5; interactive shared secret g^{ab} , or abP) , the second element (Fig 4, Fig 5; second random element b) and the first element (Fig 4, Fig 5; first intermediate shared secret $g^{a,}$ or aP) respectively (Fig 4 and Fig 5; Par 0024, 0030, 0033)

outputs the first, second and third verification parameters (Fig 4 and Fig 5; Par 0024-0025, 0030-0033; outputting interactive shared secret, second and first intermediate shared secret components).

Gentry et al '554 fails to disclose expressly

the first, second and third verification parameters for use by the third party in proving the association between the first and second parties .

however, Boneh et al discloses the first, second and third verification parameters for use by the third party in proving the association between the first and second parties (Par 0046, 0053, 0060-0063; PKG conducting authentication/ bilinear mapping based on parameter, master key, and ID).

Furthermore, Gentry et al' 885 discloses the first, second and third verification parameters for use by the third party in proving the association between the first and second parties (Par 0049-0053; 0085, 0135-0136; Claims 15-40, 56-65).

Gentry et al' 885 , Boneh et al and Gentry et al '554are analogous art because they are from the same field of authentication based on identity and bilinear mapping . At the time of invention, it will be obvious to a person of ordinary skill in the art to combine the teaching of Boneh et al ands Gentry et al' 885 with Gentry et al '554 to use the first, second and third verification parameters for use by the third party in proving the association between the first and second parties in order to provide a alternative third party authentication.

Regarding claim 2, it is rejected applying same as above applied rejecting claim 1, furthermore, Boneh et al discloses method a wherein the second party generates a further shared secret from the second secret and an identifier string of a fourth party, the second party passing this further shared secret to the fourth party for use by the latter as the private key of a public/private key pair the public key of which is formed by the identifier string of the fourth party (Par 0046, 0053, 0060-0063; association between multiple parties based on plurality of ID's and private keys).

Regarding claim 3, Gentry et al '554discloses a method wherein the first and second parties are respectively parent and child trusted authorities in a hierarchy of trusted authorities (Par 0003, 0004; trusted party).

Regarding claim 4, Gentry et al '554discloses a method wherein the first and second algebraic groups are the same (Par 0019; algebraic groups).

Regarding claim 5, Gentry et al '554discloses a method wherein the first and second elements are points on the same elliptic curve (Par 0019; elliptic curves)

Regarding claims 8, it is rejected applying as same motivation applied above rejecting claim 1, furthermore, Gentry et al '554 discloses a method/ apparatus/ computer program product of verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group; the first and second elements being such that there exists a bilinear mapping p for these elements; the method comprising a third party computer entity carrying out the following operations:

receiving data indicative of said first element (Fig 4, Fig 5; g or P) , and a first product (Fig 4, Fig 5; first intermediate shared secret g^a or aP) formed by the first party from a first secret and the first element (Fig 4 and 5; Par 0024, 0030, 0033; receiving/ generating first intermediate shared secret; PKG knowing secret components);

receiving in respect of the second party both an identifier string (Par 0022-0024; identity, or system parameters, or S_{AB} , and first (Fig 4, Fig 5; symmetric key from g^{ab}, or abP), second (Fig 4,

Fig 5; second random element b) and third (Fig 4, Fig 5; first intermediate shared secret g^{a} or aP) verification parameters (Par 0022-0024, 0030, 0033; also first random secret, second random secrets and system parameter can be interpreted as first, second and third verification parameter respectively);

computing the second element from the identifier string of the second party (Par 0022,0030; second random element);

carrying out a first check: p (third verification parameter, computed second element)=p (first element, second verification parameter) (Par 0028- 0034; determining and checking first MAC)

carrying out a second check: p (first element, first verification parameter)=p (first product, second verification parameter) (Par 0028- 0034, determining and checking second MAC)

the association between the first and second parties being treated as verified if both checks are passed (Par 0028, 0033; authentication).

Gentry et al '554 fails to disclose a third party computer entity carrying out the above checking operations.

However, Boneh et al discloses a third party carrying out a first check: p (third verification parameter, computed second element)=p (first element, second verification parameter) (Par [0053]-[0063]; claims 36-38; PKG conducting authentication based on parameter, master key, and ID); and the association between the first and second parties being treated as verified if check is passed (Par 0053-0063; claims 36-38; PKG conducting authentication based on parameter, master key, and ID).

Furthermore, Gentry et al' 885 discloses receiving in respect of the second party both an identifier string, and first, second and third verification parameters (Par 0049-0053; 0085, 0135, 0140); and

a third party carrying out a first check: p (third verification parameter, computed second element)=p (first element, second verification parameter) (Par 0049-0053; 0085, 0135-0137; PKG / root carrying out and comparing signatures/ hash functions, H)

carrying out a second check: p (first element, first verification parameter)=p (first product, second verification parameter) (Par 0049-0053; 0085, 0135; PKG / root carrying out and comparing signatures/ hash functions, H)

the association between the first and second parties being treated as verified if both checks are passed (Par 0049-0053; 0085, 0135-0136; Claims 15-40, 56-65; PKG / root carrying out and comparing signatures/ hash functions, H for authentication)

Regarding claims 9-11, they recite the limitations of claims 4-5 and 8, therefore, they are rejected applying as above rejecting claims 4-5 and 8.

Regarding claim 19, it recites the limitations of claim 1, therefore, it is rejected applying as above rejecting claim 1, furthermore, Gentry et al '554 discloses apparatus arranged to enable a third party to verify an association between the apparatus and a first party that has a first secret and is associated with a first element of a first algebraic group, the apparatus being associated with a second element, of a second algebraic group, and the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

a memory for holding a second secret and an identifier string associated with the apparatus (Par 0010-0011; system memory for storing secret, and identifying string, parameters),

means for forming said second element from said identifier string using a hash function (Par 0010, 0022,0041; processor for computing hash functions),

means for receiving from the first party a shared secret based on said first secret and said first element, and for storing this shared secret in the memory (Par 0010-0011; communicating second entities, or PKG),

means for computing first, second and third verification parameters as the product of the second secret with said shared secret, said second element and said first element respectively (Par 0030-0033, 0041; processor/ system/ PKG for receiving first random secret, second random secrets and system parameter)

Gentry et al '554 fails to disclose expressly means for making available said identifier string and said verification parameters to the third party.

However, Boneh et al discloses means for making available said identifier string and said verification parameters to the third party (Par [0053]-[0063]; PKG knowing and receiving secrets and components).

Regarding claims 20-24, they recite the limitations that already addressed in rejecting claims 1-5, 8-11 and 19, therefore, they are rejected applying as same as applied above rejecting claims 1-5, 8-11 and 19.

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from

the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

9. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136